PRIVACY AND SECURITY BY DESIGN

(PRIVACIDAD Y SEGURIDAD EN EL DISEÑO)

Trabajo de Fin de Grado en Ingeniería del Software

UNIVERSIDAD COMPLUTENSE
MADRID

Departamento de Arquitectura de Computadoras y Automática

Facultad de Informática, Junio 2017

Autor: Alicia Rodríguez Fernández-Torija

Directora: Doctora Sara Román

Agradecimientos

Primero y ante todo, me gustaría dar las gracias a Sara, mi tutora por confiar en mi, por permitirme realizar un proyecto de fin de grado no muy típico, por su dedicación, motivación y por la ayuda prestada.

Segundo, pero no menos importante, me gustaría dar las gracias a mi familia, en especial a mi madre, y a mis amigos y compañeros, tanto de curso como de trabajo por su paciencia y apoyo incondicional.

Índice

1. Resumen

Este proyecto aborda el diseño de una metodología para la realización de la evaluación de impacto a la protección de datos, que partiendo de la guía elaborada por la Agencia Española de Protección de datos a tal efecto, incorpora como requisitos de seguridad de los datos, aquellos obtenidos a partir de un análisis de riesgos realizado en base a las normas ISO 27001 (1) e ISO 27002 (2).

El proyecto implementa una solución para la parte de seguridad que ya contempla el enfoque a riesgos que propone el nuevo Reglamento Europeo de Protección de datos (R 679/2016) cuya entrada en vigor será en mayo de 2018 (3).

El proyecto presenta un modelo conceptual que recoge los requisitos funcionales de la solución, estructurada en fases y que cuenta con roles relacionados entre sí en un diagrama de flujo.

Además, como ejemplo de implementación de la solución propuesta, se ha desarrollado una herramienta web para ayudar, tanto a empresas como a administraciones, a completar el informe de evaluación de impacto a la protección de datos, que contiene las fases de la metodología junto con la identificación de riesgos y el tratamiento de los mismos.

2. Palabras Clave

Protección de datos

Privacidad

Seguridad de la información

Evaluación al impacto de la protección de datos

Reglamento europeo de protección de datos

Tratamiento de datos

Análisis de riesgos

Cumplimiento Normativo

Datos de carácter personal

Estudio previo al impacto

3. Abstract

This project is about the design of a methodology for the accomplishment of the Privacy Impact Assessment (PIA) (4), which, based on the guide developed by the Spanish Agency for Data Protection, incorporates as data security requirements those obtained from a risk analysis carried out on the basis of ISO 27001 (1) and ISO 27002 (2) standards. This project implements a solution for the security part that already contemplates the risk approach proposed by the new European Data Protection Regulation (R 679 2016) which will come into force in May 2018 (3).

The project presents a conceptual model that includes the functional requirements of the solution, structured in phases and with roles related in a flow diagram.

In addition, as an example of the proposed solution implementation, a web tool has been developed to help, companies and public administrations, to complete the Privacy Impact Assessment report, which contains the phases of the methodology as well as the risks identification and treatment.

4. Key Words

Privacy

Data protection

Security of the information

Privacy Impact Assessment

European Data Protection Regulation

Privacy risks

Risk management methodologies

Normative compliance

Personal data

Privacy by design

5. Introducción

La nueva normativa europea de protección de datos recoge, como uno de los requisitos para llevar a cabo una correcta protección de los datos de carácter personal, la realización de un estudio previo del impacto que, sobre el derecho fundamental a la protección de datos, va a implicar el nuevo tratamiento realizado por organismos públicos y privados.

Esta evaluación previa, incluida en la fase de concepción y definición del tratamiento, ayuda a prevenir posibles vulneraciones de este derecho fundamental de las personas físicas.

Por otro lado, en materia de seguridad de la información, existen diferentes marcos de control que establecen las medidas de seguridad aplicables a los sistemas de información, como es el caso de la norma ISO/IEC 27002 o su transposición a norma española UNE-ISO/IEC 27002. Estas normas se aplican también a la tipología de información como son los datos de carácter personal.

5.1 Plan de trabajo

El proyecto que nos ocupa pretende, aprovechando este nuevo requisito en materia de protección de datos y la cada vez más implantada Norma ISO/IEC 27002, la integración en una sola metodología y herramienta de la privacidad y la seguridad real en las organizaciones, conceptos muy relacionados y que, cuando se tienen en cuenta en las fases iniciales del ciclo de vida de los sistemas de información, consiguen tratamientos con un mayor nivel de cumplimiento de las normativas vigentes en materia de Seguridad de la Información y la Protección de Datos.

La herramienta planteada, **"Privacidad y seguridad en el diseño"** resulta de utilidad para cualquier tipo de organización ya que con su utilización se obtendrían beneficios relacionados con el incremento de la confianza de los clientes o ciudadanos y los propios empleados de los organismos, sabiendo que sus datos personales son tratados con un elevado nivel de privacidad y de seguridad.

5.2 Objetivo

Diseñar y desarrollar una metodología para la realización de la **Evaluación de impacto de la protección de datos personales y la seguridad de los mismos** que integra, con los requisitos de la normativa de protección de datos, los controles de la Norma ISO/IEC 27002:2013, teniendo en cuenta la Norma ISO/IEC 27001:2013 y una herramienta con tecnología web que la implemente.

5.3 Alcance

Esta metodología se podrá aplicar en cualquier organización pública o privada que diseñe un sistema de información, o modificación sustancial del mismo, e implique el tratamiento de datos de carácter personal, y puede implicar un riesgo considerable para la privacidad de las personas.

5.4 Consideraciones iniciales

Este proyecto se ha realizado cuando existe una situación transitoria en materia de protección de datos: todavía está vigente la Ley Orgánica 15/1999, pero ya está publicado el nuevo reglamento europeo de protección de datos.

Para la definición de la solución se va tener en cuenta lo que hay que cumplir actualmente salvo en el apartado de Seguridad, donde ya se va a implementar el artículo 35 del nuevo reglamento, es decir, la seguridad en base a los riesgos identificados. También se podrán tener en cuenta algunos aspectos de la nueva normativa europea para enriquecer el proyecto.

¿Cómo se identifican los riesgos?

Para ello se utilizará la técnica por excelencia que son los llamados análisis de riesgos. Se puede definir un **análisis de riesgos** como "*un proceso que comprende la identificación de activos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo"* (5).

Estos controles o medidas, después de que la Dirección defina el nivel de riesgo aceptable, conformarán la declaración de aplicabilidad del tratamiento, también conocido como SOA, siglas de Statement of Applicability. Esta declaración de aplicabilidad establece los controles que la organización debe implantar para asegurar la seguridad de toda la información que maneja. En el Anexo A de la Norma ISO 27001 se incluye un listado de los controles mínimos que las empresas deben considerar.

De todas formas, esta solución se va a desarrollar para que sea fácilmente modificable cuando entre en vigor el nuevo reglamento, ya que habrá que cambiar los actuales principios y derechos por los de la nueva legislación ya que la parte de seguridad, que en principio es lo más complicado, ya se va a tener en cuenta desde el diseño de la solución.

6. Introduction

The new European data protection legislation includes, as one of the requirements to carry out a proper protection of personal data, a preliminary study of the impact that, on the fundamental right to data protection, is going to involve the new treatment carried out by public and private administrations.

This prior evaluation, included in the conception and definition phase of the treatment, helps prevent possible violations of this fundamental right of citizens.

On the other hand, in terms of information security, there are different control frameworks that establish the security measures applicable to information systems, as in the case of ISO / IEC 27002 or its transposition into Spanish standard UNE-ISO / IEC 27002. These standards also apply to the typology of information such as personal data.

6.1 Work planning

The project in question aims, taking advantage of this new requirement in terms of data protection and the increasingly implemented ISO / IEC 27002 Standard, the integration into a single methodology and tool of privacy and real security in organizations, very concepts Related issues and that, when taken into account in the initial stages of the information systems life cycle, they achieve treatments with a higher level of compliance with the current regulations on Information Security and Data Protection.

The tool, "Privacy and security in design", is useful for any type of organization, since its use would bring benefits related to the increase of the trust of clients or citizens and the employees themselves, knowing that your personal data is treated with a high level of privacy and security.

6.2 Goals

Design and develop a methodology for carrying out the Privacy Impact Assessment (PIA) and its security, which integrates, with the requirements of data protection regulations, the controls of ISO / IEC 27002: 2013, taking into account the ISO / IEC 27001: 2013 Standard and a tool with web technology that implements it.

6.3 Scope

This methodology may be applied in any public or private organization that designs an information system, or creates substantial modification of it, and involves the processing of any personal data, and may involve a considerable risk to the privacy of citizens.

6.4 Initial Considerations

This project is been made when there is a transient situation in terms of data protection: Organic Law 15/1999 is still in force, but the new European data protection regulation is already published.

In order to define the solution, it is necessary to take into account what needs to be accomplished for the time being, except in the Security section, where Article 35 of the new regulation will already be implemented, ie security based on identified risks. It will also be possible to take into account some aspects of the new European legislation to enrich the project.

How to identify risks?

This will be the technique used for excellence that are called risk analysis. A risk analysis by definition is "*The process that involves the identification of assets, their vulnerabilities and threats to which they are exposed as well as their probability of occurrence and the impact of them in order to determine the appropriate controls to accept, decrease, transfer or avoid the occurrence of the risk*".

These controls or measures, after the Management defines the level of acceptable risk, will conform the statement of applicability of the treatment, also known as SOA, acronyms of Statement of Applicability. This is a document where organizations must describe the controls they will apply to ensure the security of all their information. Annex A of ISO 27001 includes a list of minimum controls that companies should consider.

However, this solution will be developed so that it can be easily modified when the new regulation comes into force, since it will have to change the current principles and rights for those of the new legislation since the security part, which in principle is the most complicated, will already be taken into account from the design of the solution.

7. Marco normativo aplicable

7.1 Normativa nacional de Protección de Datos de carácter personal

Actualmente el marco normativo que se encuentra en vigor en nuestro país es el siguiente:

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (6)
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD) (3)

Estas normas definen conjunto de principios que confieren garantías a los titulares de los datos y a la vez son obligaciones para las entidades que manejan los datos.

A continuación se detallan las obligaciones de las organizaciones respecto al cumplimiento de la normativa vigente en materia de protección de datos, aunque, por la extensión de los mismos y que se encuentran especificados tanto en la propia LOPD como en el RDLOPD, se incluye un breve resumen de cada uno con la indicación de los artículos de referencia en ambas normas (7) (6) (8):

- Calidad de los datos (art. 4 LOPD y art. 8, 9, 10, 11 RDLOPD):
  El tratamiento debe ser legítimo, los datos deben ser adecuados, relevantes, no excesivos, exactos, completos, recogidos para una finalidad concreta….
- Derecho de información (art. 5 LOPD y art. 18, 19 RDLOPD)):
  Derecho a ser informados, previo a la recogida de los datos, de modo expreso preciso e inequívoco sobre algunas características del tratamiento.
- Consentimiento (art. 6 LOPD y art. 12, 13, 14, 15, 16, 17 RDLOPD):
  El ciudadano debe prestar su consentimiento de manera libre, inequívoca, específica e informada, pudiendo manifestar el consentimiento de forma expresa o tácitamente.
- Datos especialmente protegidos (art. 7, 8 LOPD):
  Datos sobre ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual y violencia de género.
- Seguridad de los datos (art. 9 LOPD y Título VIII RDLOPD):
  El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de seguridad, de índole técnica y organizativa, que sean necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.
- Deber de secreto (art. 10 LOPD):
  El responsable del fichero, el encargado del tratamiento y todos aquellos usuarios que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Esta obligación de secreto se mantendrá después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

- Cesiones de datos (art. 11 LOPD):
  Solo se podrán ceder datos personales para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y el cesionario con el previo consentimiento del interesado, salvo las excepciones previstas en este artículo.
- Acceso a datos por cuenta de terceros (art. 12 LOPD y art. 20, 21, 22 RDLOPD):
  La relación entre el responsable del fichero y el encargado del tratamiento debe regularse en un contrato escrito o alguna otra forma que permita acreditar su celebración.
- Transferencias internacionales de datos (art. 33, 34 LOPD y art. 65 al 70 RDLOPD):
  Comunicaciones de datos personales a terceros países, ya sea por cesión de datos o por prestación de servicios de terceros.
- Derechos ARCO (art. 15, 16, 17 LOPD y art. 23 al 36 RDLOPD):
  Son los derechos que tiene el interesado a acceder, rectificar, cancelar sus datos de carácter personal u oponerse a su tratamiento.

7.1.1 La Evaluación de Impacto a la Protección de Datos a nivel nacional

Tanto en la Ley Orgánica 15/1999 como en su reglamento de desarrollo no existe ninguna referencia a la evaluación de impacto a la protección de datos. Ahora bien, la Agencia Española de Protección de Datos, conocedora de que este aspecto de la protección de datos iba a ser incorporado al nuevo marco europeo, publicó a finales de 1014, la Guía para una Evaluación de Impacto en la protección de datos personales (4). Este documento presenta una metodología para realizar un análisis de los riesgos que, para la protección de los datos de carácter personal, supone el tratamiento de los mismos, es decir, desarrolla un método para llevar a cabo un análisis e identificación de riesgos que un sistema de información concreto, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de las personas y, tras esta primera parte, gestionar de manera eficaz dichos riesgos, seleccionando las medidas necesarias para tratarlos.

Esta actividad se debe realizar en las fases iniciales de un nuevo producto, servicio o sistema de información y así identificar y prevenir con antelación los posibles riesgos, y de esta manera evitar los costes potenciales que se darían si se tuvieran que corregir a posteriori, cuando el servicio está en marcha o, en el caso peor, cuando ya se ha vulnerado el derecho fundamental de las personas.

La Agencia Española de Protección de Datos ha concebido esta guía como un marco flexible que podrá ser adaptado a cualquier tipo de organización, además, como su propio nombre indica, es una guía, es decir, un documento que pretende ayudar a los organismos a realizar una evaluación de este tipo y que, hasta la entrada en vigor del nuevo reglamento europeo, solo es aconsejable, no obligación legal.

7.1.2 La Seguridad de los datos a nivel nacional

Como se ha señalado anteriormente, la Seguridad en el marco de la protección de datos de carácter personal está regulado en art. 9 de la LOPD y en el Título VIII RDLOPD.

Se establecen unas medidas de seguridad obligatorias en base al tipo de datos objetos del tratamiento, es decir, si el tipo de datos tratado es de nivel básico, medio o alto, se implantarán unas u otras medidas teniendo en cuenta que si un dato es de nivel medio se aplicarán también las de nivel básico y si es de nivel alto se aplicarán las de nivel básico y medio.

Estas son las siguientes (7):

Nivel BÁSICO

- **[89] Funciones y obligaciones del personal**
  - [89.1] Funciones y obligaciones de los usuarios
  - [89.2] El personal conoce las normas de seguridad
- **[90] Gestión de las incidencias**
- **[91] Control de acceso**
  - [91.1] Acceso limitado de los usuarios
  - [91.2] Relación de usuarios y privilegios
  - [91.3] Control de acceso
  - [91.4] Control del control de acceso
  - [91.5] acceso de personal ajeno
- **[92] Gestión de soportes y documentos**
  - [92.1] Etiquetado y control de acceso
  - [92.2] Salida de soportes
    - [92.2.a] autorización del responsable de la información
    - [92.2.b] registro de salida de información anexa a correos electrónicos
  - [92.3] Protección durante el transporte
  - [92.4] Destrucción o borrado
  - [92.5] Etiquetado
    - [92.5.a] etiquetado incomprensible para personas ajenas
- **[93] Identificación y autenticación**
  - [93.1] medidas de identificación y autenticación
  - [93.2] identificación singular
  - [93.3] uso de contraseñas
  - [93.4] Cambio regular de contraseñas
    - [93.4.b] cambio anual de las contraseñas
- **[94] Copias de respaldo y recuperación**
  - [94.1] realización de copias de respaldo
    - [94.1 .a] Copia semanal
  - [94.2] recuperación de datos
  - [94.3] revisión periódica de los procedimientos
    - [94.3.a] revisión semestral de los procedimientos relativos a copias de respaldo
  - [94.4] datos para pruebas
    - [94.4.a] copia de respaldo previa al uso de datos en pruebas

Nivel MEDIO

- **[95] Responsable de seguridad**
  - [95. a] designación del responsable de seguridad en el documento de seguridad
- **[96] Auditoría**
  - [96.1] Auditoría periódica
    - [96.1.a] revisión periódica del cumplimiento de la normativa
    - [96.1.b] auditoría cada dos años
  - [96.2] informe de auditoria
    - [96.2.a] adecuación de las medidas
    - [96.2.b] identificación de deficiencias o insuficiencias
    - [96.2.c] propuesta de medidas correctivas o complementarias
  - [96.3] gestión del informe de auditoria
    - [96.3.a] gestión del informe de auditoría
- **[97] Gestión de soportes y documentos**
  - [97.1] registro de entrada de soportes
  - [97.2] registro de salida
- **[98] Identificación y autenticación**
- **[99] Control de acceso físico**
- **[100] Registro de incidencias**
  - [100.1] registro de recuperación de datos
    - [100.1.a] registro de las actuaciones de recuperación de datos
  - [100.2] autorización para la recuperación de datos
    - [100.2.a] autorización previa para la recuperación de datos

Nivel ALTO

- **[101] Gestión y distribución de soportes**
  - [101.1] etiquetado de los soportes
    - [101.1.a] etiquetado incomprensible para personas ajenas
  - [101.2] cifrado de los soportes
  - [101.3] tratamiento en entornos desprotegidos
    - [101.3.a] no se tratan datos en soportes o entornos no protegidos
- **[102] Copias de respaldo y recuperación**
  - [102.a] copia en lugar diferente al del sistema de información
  - [102.b] condiciones de seguridad del lugar de almacenamiento de las copias
- **[103] Registro de accesos**
  - [103.1]elementos registrados
    - [103.1.a] identificación del usuario
    - [103.1.b] fecha y hora del acceso
    - [103.1.c] fichero accedido
    - [103.1.d] tipo de acceso
    - [103.1.e] acceso concedido o denegado
  - [103.2] accesos autorizados
    - [103.2.a] identificación del registro accedido
  - [103.3] protección de los registros
  - [103.4] retención de los registros
    - [103.4.a] retención por un mínimo de dos años
  - [103.5] revisión de los registros
    - [103.5.a] revisión mensual de los registros
    - [103.5.b] informe de actuaciones y problemas detectados
  - [103.6]exención de la obligación de registrar
    - [103.6.a] el responsable del fichero o del tratamiento es una persona física
    - [103.6.b] se garantiza que el responsable es el único que tiene acceso
- **[104] Telecomunicaciones**

7.2 Nuevo marco europeo de Protección de Datos

Después de más de 6 años de trabajos se ha publicado el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos y que deroga la Directiva 95/46/CE (3). Este hecho está ocasionado por dos motivos:

- Por un lado la distinta legislación existente en los distintos países debido a la trasposición de la directiva europea hacían que el nivel de protección de datos en los estados miembros fuese muy dispar, realidad que, con la libre circulación de los datos que se quería impulsar, causaba perjuicio en algunos países.

- Por otro lado el avance de las tecnologías, es claro que el entorno tecnológico en el año 1995, año de la anterior directiva, tiene muy poco que ver con lo que tenemos hoy en día. La universalización de Internet, la capacidad de almacenamiento, velocidad de procesamiento han tenido mucho que ver con la aparición de nuevas herramientas como son el big data, el internet de las cosas, los servicios en nube y las redes sociales, entre otros, hacen que el entorno actual sea radicalmente distinto y el valor de los datos crece exponencialmente.

Este Reglamento ha tratado de aunar las distintas normativas de los países miembros tratando de incorporar lo mejor de cada una y, por supuesto, teniendo en cuenta el estado de la tecnología, de forma que no se ignorasen soluciones que ya están en el mercado y tendencias del mismo.

La entrada en vigor de este reglamento se producirá el 25 de mayo de 2018.

7.2.1 La Evaluación de Impacto a la Protección de Datos en el Reglamento Europeo

Uno de los aspectos que no contemplaba la Ley Orgánica 15/1999 es la Evaluación de Impacto a la Protección de Datos, este principio ya se aplicaba en otros países de la Unión Europea y es conocido como PIA, siglas de Privacy Impact Assessments, así conocidos en los países de lengua inglesa donde nacieron.

Este principio ha sido incorporado en los artículos 35 y 36 de la Sección 3 del nuevo Reglamento (3):

Artículo 35

Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si no ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, u
c) Observación sistemática a gran escala de una zona de acceso público

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36
Consulta Previa

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento

d) en su caso, los datos de contacto del delegado de protección de datos

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

7.2.2 La Seguridad de los Datos Personales en el Reglamento Europeo

El principio de Seguridad cambia radicalmente en este reglamento, como no podía ser de otra forma, ya que adopta la máxima de implantar las medidas de seguridad necesarias en cada organización teniendo en cuenta los riesgos a los que está expuesta, es decir, ya no se trata de implantar una serie de medidas igual para todas las organizaciones, sino que en base a los riesgos detectados y en base al nivel de riesgo asumible por la organización se seleccionarán e implantarán las medidas de seguridad más adecuadas.

Este aspecto está recogido en la sección 2, artículo 32 del reglamento europeo (3):

Artículo 32

Seguridad del tratamiento

1.Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

7.3 Norma ISO/IEC 27001:2013

La Norma ISO/IEC 27002 (1) proporciona un estándar para la seguridad de la información que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002 que se describe en el siguiente apartado.

7.4 Norma ISO/IEC 27002:2013

La Norma ISO/IEC 27002 (2) proporciona una serie de recomendaciones de las mejores prácticas para gestionar la seguridad de la información en cualquier organización.

La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión actual es de 2013, que sustituyó a la anterior de 2005, y que está estructurada en 14 dominios (2):

1. Políticas de Seguridad. Sobre las directrices y conjunto de políticas para la seguridad de la información. Revisión de las políticas para la seguridad de la información.

2. Organización de la Seguridad de la Información. Trata sobre la organización interna: asignación de responsabilidades relacionadas a la seguridad de la información, segregación de funciones, contacto con las autoridades, contacto con grupos de interés especial y seguridad de la información en la gestión de proyectos.

3. Seguridad de los Recursos Humanos. Comprende aspectos a tomar en cuenta antes, durante y para el cese o cambio de trabajo. Para antes de la contratación se sugiere investigar los antecedentes de los postulantes y la revisión de los términos y condiciones de los contratos. Durante la contratación se propone se traten los temas de responsabilidad de gestión, concienciación, educación y capacitación en seguridad de la información. Para el caso de despido o cambio de puesto de trabajo también deben tomarse medidas de seguridad, como lo es deshabilitación o actualización de privilegios o accesos.

4. Gestión de los Activos. En esta parte se toca la responsabilidad sobre los activos (inventario, uso aceptable, propiedad y devolución de activos), la clasificación de la información (directrices, etiquetado y manipulación, manipulación) y manejo de los soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito).

5. Control de Accesos. Se refiere a los requisitos de la organización para el control de accesos, la gestión de acceso de los usuarios, responsabilidad de los usuarios y el control de acceso a sistemas y aplicaciones.

6. Cifrado. Versa sobre los controles como políticas de uso de controles de cifrado y la gestión de claves.

7. Seguridad Física y Ambiental. Habla sobre el establecimiento de áreas seguras (perímetro de seguridad física, controles físicos de entrada, seguridad de oficinas, despacho y recursos, protección contra amenazas externas y ambientales, trabajo en áreas seguras y áreas de acceso público) y la seguridad de los equipos (emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado, mantenimiento de equipos, salida de activos fuera de las instalaciones, seguridad de equipos y activos fuera de las instalaciones, reutilización o retiro de equipo de almacenamiento, equipo de usuario desatendido y política de puesto de trabajo y bloqueo de pantalla).

8. Seguridad de las Operaciones: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.

9. Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información.

10. Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.

11. Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.

12. Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.

13. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.

14. Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

5. POLÍTICAS DE SEGURIDAD

5.1 Directrices de gestión de la seguridad de la información

5.1.1 Las políticas de seguridad de la información

5.1.2 Revisión de las políticas de seguridad de la información

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Organización interna

6.1.1 Roles y responsabilidades en seguridad de la información

6.1.2 Segregación de tareas

6.1.3 Contacto con las autoridades

6.1.4 Contacto con grupos de interés especial

6.1.5 Seguridad de la información en la gestión de proyectos

6.2 Los dispositivos móviles y el teletrabajo

6.2.1 Política de dispositivos móviles

6.2.2 Teletrabajo

7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

7.1 Antes del empleo

7.1.1 Investigación de antecedentes

7.1.2 Términos y condiciones del empleo

7.2 Durante el empleo

7.2.1 Responsabilidades de gestión

7.2.2 Concienciación, educación y capacitación en seguridad de la información

7.2.3 Proceso disciplinario

7.3 Finalización del empleo o cambio en el puesto de trabajo

7.3.1 Responsabilidades ante la finalización o cambio

8. GESTIÓN DE ACTIVOS

8.1 Responsabilidad sobre los activos

8.1.1 Inventario de activos

8.1.2 Propiedad de los activos

8.1.3 Uso aceptable de los activos

8.1.4 Devolución de activos

8.2 Clasificación de la información

8.2.1 Clasificación de la información

8.2.2 Etiquetado de la información

8.2.3 Manipulado de la información

8.3 Manipulación de los soportes

8.3.1 Gestión de soportes extraíbles

8.3.2 Eliminación de soportes

8.3.3 Soportes físicos en tránsito

9. CONTROL DE ACCESOS

9.1 Requisitos de negocio para el control de acceso

9.1.1 Política de control de acceso

9.1.2 Acceso a las redes y a los servicios de red

9.2 Gestión de acceso de usuario

9.2.1 Registro y baja de usuario

9.2.2 Provisión de acceso de los usuarios

9.2.3 Gestión de privilegios de acceso

9.2.4 Gestión de la información secreta de autenticación de usuarios

9.2.5 Revisión de los derechos de acceso de usuario

9.2.6 Retirada o reajuste de los derechos de acceso

9.3 Responsabilidad del usuario

9.3.1 Uso de la información secreta de autenticación

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricción del acceso a la información

9.4.2 Procedimientos seguros de inicio de sesión

9.4.3 Sistemas de gestión de contraseñas

9.4.4 Uso de las utilidades con privilegios del sistema

9.4.5 Control de acceso al código fuente de los programas

10. CRIPTOGRAFÍA

10.1 Controles criptográficos

10.1.1 Política de uso de los controles criptográficos

10.1.2 Gestión de claves

11. SEGURIDAD FÍSICA Y DEL ENTORNO

11.1 Áreas seguras

11.1.1 Perímetro de seguridad física

11.1.2 Controles físicos de entrada

11.1.3 Seguridad de oficinas, despachos y recursos

11.1.4 Protección contra las amenazas externas y ambientales

11.1.5 El trabajo en áreas seguras

11.1.6 Áreas de carga y descarga

11.2 Seguridad de los equipos

11.2.1 Emplazamiento y protección de equipos

11.2.2 Instalaciones de suministro

11.2.3 Seguridad del cableado

11.2.4 Mantenimiento de los equipos

11.2.5 Retirada de materiales propiedad de la empresa

11.2.6 Seguridad de los equipos fuera de las instalaciones

11.2.7 Reutilización o eliminación de equipos

11.2.8 Equipo de usuario desatendido

11.2.9 Política de puesto de trabajo despejado y pantalla limpia

12. SEGURIDAD DE LAS OPERACIONES

12.1 Procedimientos y responsabilidades operacionales

12.1.1 Documentación de procedimientos de operación

12.1.2 Gestión de cambios

12.1.3 Gestión de capacidades

12.1.4 Separación de los recursos de desarrollo, prueba y producción

12.2 Protección contra software malicioso

12.2.1 Controles contra el código malicioso

12.3 Copias de seguridad

12.3.1 Copias de seguridad de la información

12.4 Registros y supervisión

12.4.1 Registro de eventos

12.4.2 Protección de la información de registro

12.4.3 Registros de administración y operación

12.4.4 Sincronización del reloj

12.5 Control del software en explotación

12.5.1 Instalación del software en explotación

12.6 Gestión de la vulnerabilidad técnica

12.6.1 Control de las vulnerabilidades técnicas

12.6.2 Restricción en la instalación de software

12.7 Consideraciones sobre la auditoría de sistemas de información

12.7.1 Control de auditoría de sistemas de información

13. SEGURIDAD DE LAS COMUNICACIONES

13.1 Gestión de la seguridad de redes

13.1.1 Controles de red

13.1.2 Seguridad de los servicios de red

13.1.3 Segregación en redes

13.2 Intercambio de información

13.2.1 Políticas y procedimientos de intercambio de información

13.2.2 Acuerdos de intercambio

13.2.3 Mensajería electrónica

13.2.4 Acuerdos de confidencialidad

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SI

14.1 Requisitos de seguridad en sistemas de información

14.1.1 Análisis de requisitos y especificaciones de Seguridad de la información

14.1.2 Asegurar los servicios de aplicaciones en redes públicas

14.1.3 Protección de las transacciones de servicios de aplicaciones

14.2 Seguridad en desarrollo y proceso de soporte

14.2.1 Política de desarrollo seguro

14.2.2 Procedimiento de control de cambios en sistemas

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el s. operativo

14.2.4 Restricciones a los cambios en los paquetes de software

14.2.5 Principios de ingeniería de sistemas seguros

14.2.6 Entorno de desarrollo seguro

14.2.7 Externalización del desarrollo de software

14.2.8 Pruebas funcionales de seguridad

14.2.9 Pruebas de aceptación de sistemas

14.3 Datos de prueba

14.3.1 Protección de los datos de pruebas

15. RELACIÓN CON PROVEEDORES

15.1 Seguridad en la relación con proveedores

15.1.1 Política de seguridad de la información en relaciones con los proveedores

15.1.2 Requisitos de seguridad en contratos con terceros

15.1.3 Cadena de suministro de tecnologías de la información y comunicaciones

15.2 Gestión de la provisión de servicios del proveedor

15.2.1 Supervisión y revisión de los servicios prestados por terceros

15.2.2 Gestión de cambios en los servicios prestados por terceros

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 Gestión de incidentes de seguridad de la información y mejoras

16.1.1 Responsabilidades y procedimientos

16.1.2 Notificación de los eventos de seguridad de la información

16.1.3 Notificación de puntos débiles de la seguridad

16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información

16.1.5 Respuesta a los incidentes de seguridad de la información

16.1.6 Aprendizaje de los incidentes de seguridad de la información

16.1.7 Recopilación de evidencias

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

17.1 Continuidad de la seguridad de la información

17.1.1 Planificación de la continuidad de la seguridad de la información

17.1.2 Implementar la continuidad de la seguridad de la información

17.1.3 Pruebas, mantenimiento y reevaluación de planes continuidad del negocio

17.2 Redundancias

17.2.1 Disponibilidad de instalaciones de tratamiento de la información

18. CUMPLIMIENTO

18.1 Cumplimiento de los requisitos legales

18.1.1 Identificación de la legislación aplicable

18.1.2 Derechos de propiedad intelectual (DPI)

18.1.3 Protección de los registros de la organización

18.1.4 Protección de datos y privacidad de la información de carácter personal

18.1.5 Regulación de los controles criptográficos

18.2 Revisión de la seguridad de la información

18.2.1 Revisión independiente de la seguridad de la información

18.2.2 Cumplimiento de las políticas y normas de seguridad

18.2.3 Comprobación del cumplimiento técnico

8. Descripción de la solución propuesta

La Guía para la Evaluación de Impacto en la Protección de Datos Personales, EIPD, es un documento publicado por la Agencia Española de Protección de Datos (4) a finales del 2014, que presenta una metodología para realizar un análisis de los riesgos que, para la protección de los datos de carácter personal, supone el tratamiento de los mismos. La solución propuesta está basada en esta Guía, aunque teniendo en cuenta el nuevo Reglamento Europeo y con el cambio fundamental de la seguridad de los datos.

El proyecto consta de dos partes:

- **Diseño y desarrollo de la metodología.**
  Esta parte teórica consistirá en adaptar y simplificar la metodología que contempla la Evaluación de impacto en la protección de datos de carácter personal de la Agencia Española de Protección de Datos, con la seguridad global de los mismos, partiendo de la metodología definida en la Guía de EIPD.

  En esta fase se realizará un estudio inicial de los requisitos exigidos por la normativa española y por la Norma ISO/IEC 27002:2013 y que afectan a la seguridad de los datos de carácter personal y se incorporarán, según proceda, a las fases anteriores. Como consecuencia de esta parte del proyecto podrán resultar nuevas fases, eliminación de fases y/o modificación de alguna de las existentes.

  En esta parte del proyecto se describirá en que consiste en cada una de las fases de la metodología resultante, en base al cambio de requisitos de seguridad, es decir, el cambio de las medidas del Título VIII de las medidas de seguridad en el tratamiento de datos de carácter personal, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal por un marco más amplio que contenga las anteriores, como son las establecidas en la propia Norma ISO/IEC 27002:2013.

- **Diseño y desarrollo de la Herramienta Privacy and Security by Desing**
  Esta parte práctica del proyecto consistirá en el diseño y desarrollo de una solución web que implemente la metodología diseñada en el modelo conceptual anteriormente expuesto.

  Con esta herramienta, el equipo responsable de esta tarea en la organización podrá realizar el informe que recoja el impacto que un tratamiento de datos de carácter personal pueda tener para la Protección de los Datos de carácter personal y la Seguridad de los mismos.

8.1 Primera parte: Modelo conceptual

8.1.1 Requisitos funcionales generales

Los requisitos funcionales, a tratarse del desarrollo de una solución para dar cumplimiento a un requisito legal, son los propios de las normas citadas en el apartado 6 de este documento.

8.1.2 Roles intervinientes en un EIPD

La Guía de la AEPD, propone la creación de un grupo multidisciplinar para la realización de la EIPD, grupo de trabajo compuesto por personal de los diferentes departamentos de la organización que tengan relación directa con el tratamiento objeto de la evaluación. La propia Agencia no establece de forma fija quienes deben pertenecer a este grupo, ya que lo deja abierto dependiendo de muchos factores: el tamaño de la organización, su estructura organizativa, el negocio al que se dedique y su idiosincrasia. Respecto a este último punto incidir que lo que para una organización funcionaría perfectamente, para otra no, aunque sean de tamaños similares, estructuras parecidas y negocios similares: la cultura de la organización es un punto fundamental a tener en cuenta como CLAVE de ÉXITO del proyecto.

En este apartado también se va a incluir alguno de los enfoques del nuevo reglamento europeo y directrices de la propia Agencia Española de Protección de Datos relacionados con el Delegado de Protección de Datos, DPD, también conocido por DPO por sus siglas en inglés, Data Protection Officer. Esta figura, ya implantada desde hace años en otros países, está definida en la sección 4 del Reglamento.

En este proyecto se propone crear una estructura de roles sencilla, aunque para alguna de las fases del proyecto y dependiendo de la envergadura del mismo, el responsable del fichero deba solicitar información o ayuda a otros departamentos de la organización, como puede ser el departamento jurídico, el de personal, etc….

Los roles propuestos son los siguientes:

- **Equipo de protección de datos:** Este equipo estará compuesto por los especialistas de protección de datos de la organización, podría depender del Delegado de Protección de Datos, y serían los usuarios que harían uso de la metodología y la herramienta objeto del proyecto.

- **Responsable del fichero/tratamiento:** La definición de responsable se define en la LOPD, en su reglamento de desarrollo y en el nuevo reglamento europeo. Vamos reflejar aquí en esta última definición: *"Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento…."*
  Es decir, será el que decida qué datos se recogerán para el tratamiento y cómo se van a tratar. Al ser este el que tenga conocimiento del negocio, deberá proporcionar la información necesaria al equipo de protección de datos para que pueda realizar una correcta EIPD, y para ello, y dependiendo del supuesto concreto, podrá solicitar ayuda a otros departamentos de la organización, tal y como se ha indicado anteriormente.

- **Equipo de seguridad TIC:** Este equipo estará compuesto por perfiles TIC expertos en análisis de riesgos informáticos. Son los responsables de la realización de los análisis de riesgos de los Sistemas de Información asociados a los tratamientos objeto del EIPD.
  Para este análisis de riesgos, este equipo se deberá basar en una metodología formal y utilizar, si es posible, una herramienta automatizada de las existentes en el mercado, ya que, si se precisa de un EIPD, es porque el tratamiento no es sencillo y por tanto, la posibilidad que recoge el nuevo reglamento europeo de utilizar un método informal para realizar el análisis de riesgos no tiene cabida en este proyecto.
  Este equipo realizará el informe de análisis de riesgos del tratamiento basado en la Norma ISO 27002, donde se indicarán los riesgos para la seguridad de los datos personales y los tratamientos de los mismos que indican los controles de esa norma que se aconseja implementar o modificar su implementación.

8.1.3 Fases de la metodología propuesta

Esta metodología estará basada en un ciclo PDCA (***plan-do-check-act***, esto es, **planificar-hacer-verificar-actuar**), por la propia finalidad de esta metodología. No se trata solo de prever los posibles riesgos a la protección de datos que puede tener un nuevo tratamiento o una modificación sustancial de uno ya existente, sino también de identificar, para esos riesgos, el tratamiento que se le va a dar a cada uno de ellos y realizar un análisis de cumplimiento, para, con toda esta información elaborar el informe final que se debe entregar al Responsable del Fichero o tratamiento.

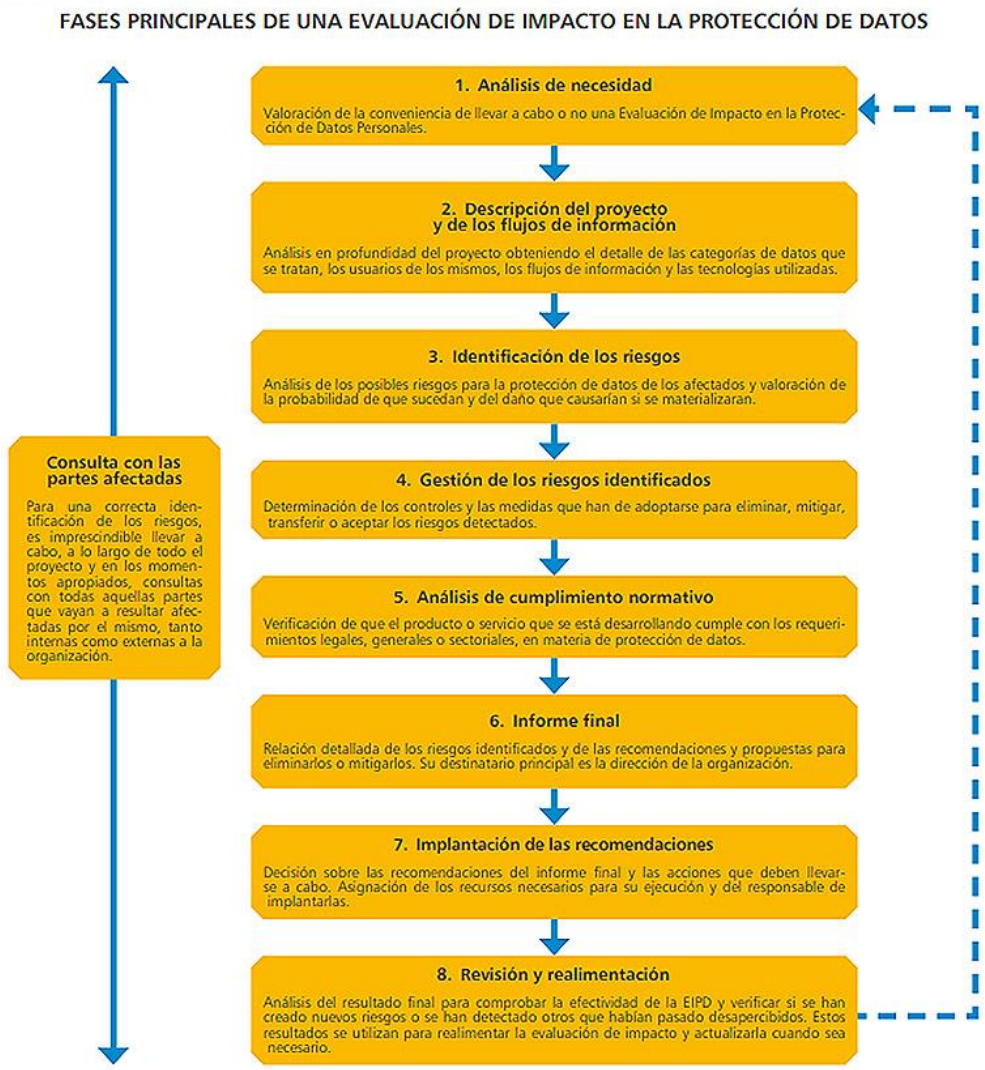
La solución contempla la elaboración del informe de EIPD, aunque necesitará de resultados de otras actividades realizadas por otras partes de la organización para la realización del mismo:

- El análisis de riesgos será realizado por el equipo de seguridad y los resultados se incluirán en la fase de identificación de los riesgos.

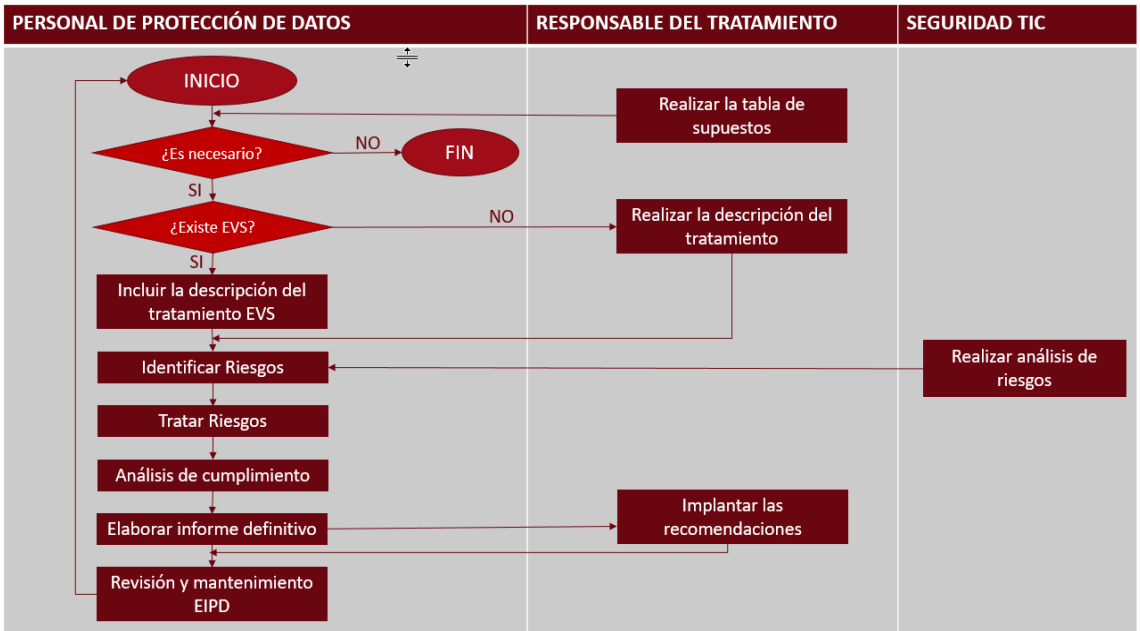
- La descripción del tratamiento, si ya se ha realizado un Estudio de Viabilidad del Sistema, se podrá extraer esta información de ahí. En caso de que no existiera este documento previo, serán los gestores o el personal informático encargado de la aplicación, los que tendrán que suministrar esta información.

En la guía de la Agencia Española de Protección de Datos (4) hay ocho fases obligatorias y claramente diferenciadas, la innovación en este proyecto implica la diferenciación de fases por actores y los puntos anteriormente citados.

Gráficamente en la Guia de la Agencia (4):



Gráficamente la solución propuesta:



Necesidad de realización de un EIPD

En primer lugar habrá que considerar la necesidad de realizar el estudio previo que constituye el EIPD.

Actualmente, en la Guía de la Agencia Española de Protección de Datos, existe una serie de supuestos que implicarían la necesidad de elaborar un documento de este tipo, y se detallan en la siguiente tabla (4).

Esta tabla debería incluirse al realizar el Estudio de Viabilidad del Sistema, tanto cuando se vaya a realizar nuevo tratamiento como cuando uno ya existente vaya a sufrir una modificación sustancial.

Supuestos que aconsejan la realización de un EIPD:	
Se recogen nuevas categorías de datos personales o se hacen con ellos nuevos usos más invasivos.	
Hay un tratamiento significativo de datos de menores, especialmente de menos de catorce años.	
Evalúa o predice aspectos personales relevantes, susceptibles de configurar un perfil personal.	
Trata grandes volúmenes de datos personales con tecnologías de datos masivos (big data), internet de las cosas (Internet of things) o ciudades inteligentes (smart cities).	
Utiliza tecnologías invasivas con la privacidad: videovigilancia, aeronaves no tripuladas, minería de datos, biometría, vigilancia electrónica, técnicas genéticas, geolocalización, etc.	
Trata gran cantidad de datos de un número elevado de personas.	
Indicar el número estimado de personas a tratar:	
Se ceden o comunican datos personales a terceros.	
Transfiere datos a países que no forman parte del Espacio Económico Europeo y no han sido objeto de una declaración de adecuación por parte de la Comisión Europea o la Agencia Española de Protección de Datos.	
Utiliza formas intrusivas para contactar con las personas.	
Utiliza datos personales no disociados o no anonimizados con fines estadísticos, históricos o de investigación científica.	
Trata datos especialmente protegidos:	
Ideología, religión, creencias y afiliación sindical	
Origen racial, salud y vida sexual	
Hay riesgos que pueden comprometer la confidencialidad, integridad o disponibilidad.	
Otros motivos por los que deba realizarse una EIPD, (Evaluación del Impacto de la Protección de Datos):	

Será el equipo encargado de la realización el EIPD los que, junto con el Responsable del Fichero o tratamiento, en base a los resultados de la tabla anterior, decidan sobre la oportunidad de realizar el informe.

NOTA: Cuando sea de aplicación el nuevo reglamento, esta fase se deberá modificar ya que este reglamento contempla que sean las autoridades de control de los distintos países los que elaboren listas de tratamiento que requerirán la realización de un EIPD y listas de tratamientos que no lo requerirán.

Descripción del tratamiento

Se deberá detallar:

- Resumen ejecutivo del tratamiento
- Tipo de datos tratados
- Roles y funciones de los mismos, especificando si son personal interno o externo a la organización
- Relación entre roles y tipo de datos a los que accede
- Flujo de datos personales y su uso, identificando procedencia y destino de los mismos.
- Tecnología utilizada

NOTA: En caso de existir un Estudio de Viabilidad muchos de estos aspectos se podrán extraer del mismo.

Identificación de los riesgos a la protección de datos

Los riesgos están asociados a la falta de cumplimiento de los requisitos que impone la normativa vigente en materia de protección de datos y que ya han sido identificados en el apartado 2 de este documento.

En esta fase no solo hay que identificar los riesgos, sino también establecer, para cada uno de ellos, la probabilidad de que se materialice y su posible impacto en la organización. Esta catalogación la debe realizar el equipo de protección de datos con ayuda del responsable del fichero.

En esta fase se utilizará la tabla incluidas en la propia Guía de la AEPD, salvo los riesgos a la seguridad de los datos que serán los recogidos en la norma ISO/IEC 27002 y se indican en la fase siguiente (4).

TIPOLOGÍA	DESCRIPCIÓN DEL RIESGO	NIVEL DE IMPACTO SI EL RIESGO SE MATERIALIZA ALTO / MEDIO / BAJO	PROBABILIDAD DE QUE SE MATERIALICE ALTO / MEDIO / BAJO
Generales	Pérdidas económicas o daños reputaciones por incumplimiento de la normativa de protección de datos		
	Pérdidas económicas o daños reputaciones por incumplimiento de normas sectoriales con incidencia en la protección de datos		
	Pérdidas económicas, de clientes o daños reputaciones por falta de medidas de seguridad o ineficacia de estas.		
	Pérdidas de competitividad por daños reputaciones por una mala gestión de la privacidad		
	Falta de conocimiento experto sobre protección de datos y de canales con los afectados		
	Incorporación tardía de expertos al proyecto e indefinición de sus funciones		
Legitimación de tratamientos y cesiones	Tratar o ceder datos no necesarios para la finalidad		
	Carecer de legitimación legal para el tratamiento o cesión		
	Obtener consentimiento dudoso para el tratamiento o cesión de datos		
	Dificultar la revocación del consentimiento u oposición al tratamiento		
	Dificultades para garantizar la legitimidad de la recogida o cesión provenientes de terceros		
	Solicitar y tratar datos especialmente protegidos sin necesidad o sin medidas de seguridad		
	Enriquecer los datos iniciales sin la información adecuada a los afectados al realizar una interconexión con ficheros de terceros		
	Utilizar cookies u otros mecanismos sin autorización clara		
	Impedir la utilización anónima de un determinado producto o servicio si no es necesario		
Transferencias internacionales	Acceso secreto a datos por autoridades de terceros países		
	Carencia de mecanismos de control de cumplimiento para la transferencia de datos		
	Impedimentos por parte del receptor para realizar controles		
	Incapacidad de ayudar a los afectados para ejercitar sus derechos ante el receptor		
	No obtención de las autorizaciones legales necesarias		
Notificación de tratamientos	Carecer de procedimientos necesarios para detectar la notificación de ficheros		
Transparencia de los tratamientos	Recoger datos sin proporcionar la información necesaria		
	En entornos web colocar la información de protección de datos en lugares de difícil localización		
	Redactar información en lenguaje no claro		
Calidad de los datos	Solicitar datos innecesarios		
	Garantías insuficientes para el uso con fines históricos, estadísticos o científicos		
	Realizar deducciones erróneas mediante la utilización de técnicas de inteligencia artificial		
	Existencia de errores técnicos u organizativos que propicien falta de integridad		
	Utilizar los datos para finalidades incompatibles con la declarada		
	Indefinición para la cancelación de los datos		
Datos	Fallos o errores sistemáticos u ocasionales para recabar consentimiento expreso para el tratamiento o cesión		

TIPOLOGÍA	DESCRIPCIÓN DEL RIESGO	NIVEL DE IMPACTO SI EL RIESGO SE MATERIALIZA ALTO / MEDIO / BAJO	PROBABILIDAD DE QUE SE MATERIALICE ALTO / MEDIO / BAJO
especialmente protegidos	Asunción errónea de la existencia de habilitación legal para el tratamiento o cesión		
	Fallos para recabar el consentimiento expreso para el tratamiento o para la cesión		
Deber de secreto	Puede existir algún acceso no autorizado		
	Violaciones de confidencialidad de los datos personales por parte de los empleados		
Tratamientos por encargo	Inexistencia de contrato o elaboración del contrato incorrecto que no refleje todos los apartados necesarios o las garantías adecuadas		
	Falta de diligencia en la elección del encargado del tratamiento		
	Gestión deficiente de subcontrataciones o incorrecto seguimiento de la contratación		
	No definición o deficiencias en los procedimientos para comunicar al responsable los derechos ARCO		
	Dificultades para conseguir la portabilidad de los datos		
Derechos ARCO	Dificultar o imposibilitar el ejercicio de los derechos ARCO		
	Carencia de procedimientos y herramientas para la gestión de los derechos ARCO		
	Carencia de procedimientos para comunicar rectificaciones, cancelaciones u oposiciones a los cesionarios de datos personales		

Identificación de los riesgos a la seguridad de los datos

Estos riesgos están identificados a partir de los dominios de la norma ISO/IEC 27002 (2) y se completará la tabla con la información suministrada por el análisis de riesgos. Este análisis de riesgos se deberá realizar según el apartado 8.1.2 Apreciación de riesgos de seguridad de la información de la Norma ISO/IEC 27001 (1) .

Este apartado se deberá cumplimentar junto con el equipo de seguridad de la organización que son los que han realizado el análisis de riesgos. Como consecuencia de esta tarea se tendrá información de los controles que son de aplicación al tratamiento, esto es, el SoA.

DOMINIO	DESCRIPCIÓN DEL RIESGO	NIVEL DE IMPACTO SI EL RIESGO SE MATERIALIZA ALTO / MEDIO / BAJO	PROBABILIDAD DE QUE SE MATERIALICE ALTO / MEDIO / BAJO
Políticas de seguridad	Falta de directrices o incorrecta definición de las mismas		
	Falta de revisiones de las directrices		
Organización de la Seguridad	Falta de definición de roles o poco clara		
	No existencia de segregación de tareas		
	No existencia de requisitos de seguridad en la gestión de proyectos		

DOMINIO	DESCRIPCIÓN DEL RIESGO	NIVEL DE IMPACTO SI EL RIESGO SE MATERIALIZA ALTO / MEDIO / BAJO	PROBABILIDAD DE QUE SE MATERIALICE ALTO / MEDIO / BAJO
	No existencia de política de dispositivos móviles		
	Si existe teletrabajo, falta de directrices de seguridad para el teletrabajo		
Seguridad relativa a los recursos humanos	Falta de controles de seguridad antes de la contratación		
	Falta de controles de seguridad durante de la contratación		
	Falta de controles de seguridad después de la contratación		
Gestión de activos	Falta de responsabilidad sobre los activos		
	No existencia de inventario de activos		
	Indefinición en la entrega y devolución de activos		
	No existencia de la clasificación de la información		
	No existencia del etiquetado de la información		
	No existencia de la gestión del ciclo de vida de los soportes		
Control de accesos	Falta de política de control de accesos		
	Indefinición de acceso a redes y servicios en red		
	Inexistencia o incorrecta gestión de los accesos de usuario		
	Falta de control en la información secreta de autenticación		
	Falta de control de acceso a sistemas y aplicaciones		
Criptografía	Inexistencia de política de controles criptográficos		
	Falta de gestión de claves o gestión inadecuada de las mismas		
Seguridad física y del entorno	No existencia de áreas seguras		
	Falta de seguridad en los equipos		
Seguridad de las operaciones	Falta o definición incorrecta de procedimientos de operación		
	Falta de gestión de cambios		
	Falta de gestión de capacidades		
	No existencia de separación de recursos de desarrollo, pruebas y operación		
	Falta de controles contra malware		
	No existencia de copias de seguridad		
	Falta de gestión de registros de eventos		
	Falta de registros de administración y operación		
	Inexistencia de sincronización de reloj		

DOMINIO	DESCRIPCIÓN DEL RIESGO	NIVEL DE IMPACTO SI EL RIESGO SE MATERIALIZA ALTO / MEDIO / BAJO	PROBABILIDAD DE QUE SE MATERIALICE ALTO / MEDIO / BAJO
	Falta de control de la instalación del software en explotación		
	Falta de gestión de vulnerabilidades		
	No existencia de instalación de software		
Seguridad en las comunicaciones	Falta de gestión de la seguridad de las comunicaciones o gestión incorrecta		
	Falta de políticas y procedimientos de intercambios de información		
	Falta de controles en la mensajería electrónica		
Adquisición, desarrollo y mantenimiento de sistemas de información	Falta de requisitos de seguridad en los sistemas de información		
	Falta de política de desarrollo seguro		
	Falta de procedimiento de control de cambios		
	Falta de revisiones técnicas tras los cambios		
	Entorno de desarrollo seguro		
	Falta de pruebas		
	Falta de protección de datos de pruebas		
Relación con proveedores	Falta de política de seguridad de la información en relaciones con los proveedores		
	Falta de requisitos de seguridad en contratos con terceros		
	Falta o inadecuada gestión de la provisión de servicios		
Gestión de incidentes de seguridad de la información	Falta o inadecuada gestión de incidentes de seguridad		
Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Inexistencia del Plan de Continuidad de Negocio		
	Falta de implementación del Plan de Continuidad de Negocio		
	Falta de mantenimiento del Plan de Continuidad de Negocio		
	Falta de pruebas de continuidad		
	Falta de centro de respaldo		
Cumplimiento	Incumplimiento de requisitos legales aplicables		
	Falta de protección de registros de la organización		
	Falta de regulación de controles criptográficos		
	Falta de revisiones de seguridad		
	Incumplimiento de políticas y normas de seguridad		

Tratamiento de los riesgos identificados

Una vez identificados los riesgos a la protección de datos en la fase anterior, lo que procede es tratarlos o gestionarlos.

El tratamiento de riesgos se produce al implantar medidas que pueden:

a) evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;

b) tomar o aumentar el riesgo con el fin de perseguir una oportunidad;

c) eliminar la fuente de riesgo;

d) los cambios en la probabilidad;

e) cambiar las consecuencias;

f) la distribución del riesgo con la otra parte o partes (incluidos los contratos y la financiación de riesgo);

g) mantener el riesgo por decisión informada.

Estas opciones de tratamiento de riesgos a considerar son las presentadas en la norma ISO 31000:2009 – Risk management. Principles and guidelines.

Para seleccionar las posibles medidas que se pueden implementar a la hora de tratar los riesgos, se van a incluir las recogidas en la Guía de la AEPD. Este será un primer catálogo que podrá ser ampliado conforme el organismo vaya adquiriendo madurez en la realización de estos informes (4).

TIPOLOGÍA	DESCRIPCIÓN DEL RIESGO	MEDIDA
Generales	Pérdidas económicas o daños reputaciones por incumplimiento de la normativa de protección de datos	Formación al personal en PD Comunicación clara y auditable de las responsabilidades relacionadas con el cumplimiento y con las consecuencias en caso de incumplimiento
	Pérdidas económicas o daños reputaciones por incumplimiento de normas sectoriales con incidencia en la protección de datos	Formación al personal en PD a nivel sectorial Comunicación clara y auditable de las responsabilidades relacionadas con el cumplimiento (sectorial) y con las consecuencias en caso de incumplimiento
	Pérdidas económicas, de clientes o daños reputaciones por falta de medidas de seguridad o ineficacia de estas.	Formación al personal en Seguridad y uso de las TIC Comunicación clara y auditable de las responsabilidades relacionadas con el cumplimiento de políticas y normas de seguridad y con las consecuencias en caso de incumplimiento
	Pérdidas de competitividad por daños reputaciones por una mala gestión de la privacidad	Formación al personal en PD, Seguridad y uso de las TIC
	Falta de conocimiento experto sobre protección de datos y de canales con los afectados	Nombramiento para la interlocución con los afectados Nombrar a un Delegado de Protección de Datos (DPO), que también puede hacer de interlocutor.
	Incorporación tardía de expertos al proyecto e indefinición de sus funciones	Incorporación de privacidad en el diseño Incorporación DPO

TIPOLOGÍA	DESCRIPCIÓN DEL RIESGO	MEDIDA
Legitimación de tratamientos y cesiones	Tratar o ceder datos no necesarios para la finalidad	Usar datos disociados Si se puede, utilizar el uso de anónimos Revisar la existencia de datos personales no utilizados Utilizar pseudónimos Evitar el uso de datos biométricos
	Carecer de legitimación legal para el tratamiento o cesión	Formación al personal en PD, Seguridad y uso de las TIC Revisar las posibilidades de legitimación para un posible encaje Buscar asesoramiento experto Si se ceden datos, establecer acuerdos escritos
	Obtener consentimiento dudoso para el tratamiento o cesión de datos	Asegurarse de que no existen otras causas de legitimación más adecuadas Si existe una relación contractual, separar los datos necesarios de los prescindibles No condicionar el uso de un servicio o producto al consentimiento para otra finalidad Evitar basar los tratamientos de datos basados en el consentimiento de los trabajadores Evitar forzar el consentimiento desde una posición de prevalencia o cuando existen causas legitimas
	Dificultar la revocación del consentimiento u oposición al tratamiento	Establecer procedimientos claros para revocar el consentimiento o solicitud de oposición. Establecer mecanismos necesarios para garantizar que se consultan ficheros de exclusión.
	Dificultades para garantizar la legitimidad de la recogida o cesión provenientes de terceros	Exigir las garantías de que los datos de terceros se han obtenido y cedido legalmente En la realización de campañas publicitarias con datos de terceros, exigir garantías de que los afectados han dado su consentimiento
	Solicitar y tratar datos especialmente protegidos sin necesidad o sin medidas de seguridad	Verificar que el tratamiento de datos especialmente protegidos es imprescindible para la finalidad Verificar que el tratamiento está amparado por la Ley En caso contrario garantizar que se obtienen el consentimiento expreso o por escrito
	Enriquecer los datos iniciales sin la información adecuada a los afectados al realizar una interconexión con ficheros de terceros	Verificar la legitimidad de la interconexión de datos prevista Definir los datos resultantes del tratamiento y verificar que no se han generado más.
	Utilizar cookies u otros mecanismos sin autorización clara	Evitar uso de cookies u otros mecanismos de rastreo y monitorización, si se utilizan escoger las menos invasivas Informar sobre el uso y finalidad de las cookies Respetar las preferencias de los afectados en sus navegadores
	Impedir la utilización anónima de un determinado producto o servicio si no es necesario	Permitir uso anónimo de servicios y productos cuando no sea necesario la identificación de las personas
Transferencias internacionales	Acceso secreto a datos por autoridades de terceros países	Incluir cláusulas de salvaguarda en las que se refiera información sobre los accesos a datos transferidos tan pronto como sea posible
	Carencia de mecanismos de control de cumplimiento para la transferencia de datos	Implantar mecanismos de control para garantizar que se cumplen las condiciones bajo las que se llevó a cabo la transferencia
	Impedimentos por parte del receptor para realizar controles	Asegurarse de la exigencia de mecanismos de control del importador
	Incapacidad de ayudar a los afectados para ejercitar sus derechos ante el receptor	Asegurarse de la definición y funcionamiento de un canal de comunicación para las solicitudes y reclamaciones Poner en marcha procedimientos que garanticen la adecuada atención de las demandas
	No obtención de las autorizaciones legales necesarias	Solicitar autorización de la Directora de la AEPD si es necesario

TIPOLOGÍA	DESCRIPCIÓN DEL RIESGO	MEDIDA
Notificación de tratamientos	Carecer de procedimientos necesarios para detectar la notificación de ficheros	Incluir en los procesos y metodologías de desarrollo tareas para notificar nuevos ficheros a la AEPD
Transparencia de los tratamientos	Recoger datos sin proporcionar la información necesaria	Informar sobre el uso y finalidad de las cookies Establecer procedimientos para la revisión de los formularios de recogida de datos que garanticen el cumplimiento de la política de privacidad, homogeneidad de la información que la información es la adecuada
	En entornos web colocar la información de protección de datos en lugares de difícil localización	Estructurar y proporcionar información en varios niveles para su fácil comprensión Verificar que la información ofrecida es consistente y coherente Verificar que la información está en todos los formularios
	Redactar información en lenguaje no claro	Implantar políticas de privacidad claras, concisas y asequibles, en formatos estandarizados y uniformes en toda la organización
Calidad de los datos	Solicitar datos innecesarios	Revisar la existencia de datos personales no utilizados
	Garantías insuficientes para el uso con fines históricos, estadísticos o científicos	Usar datos disociados Si se puede, utilizar el uso de anónimos Utilizar pseudónimos Garantizar que se aplican las medidas según el nivel de seguridad
	Realizar deducciones erróneas mediante la utilización de técnicas de inteligencia artificial	Establecer mecanismos y procedimientos para resolver rápidamente los errores Establecer vías de impugnación ágiles a los afectados Establecer canales para tratar falsos negativos y positivos en a identificación y autenticación con datos biométricos
	Existencia de errores técnicos u organizativos que propicien falta de integridad	Establecer medidas técnicas y organizativas para la actualización de datos en toda la organización
	Utilizar los datos para finalidades incompatibles con la declarada	Suministrar información clara sobre las finalidades Suministrar información sobre los criterios utilizados para la toma de decisiones Proporcionar información sobre las medidas implantadas
	Indefinición para la cancelación de oficio de los datos	Definir plazos de cancelación Establecer controles automáticos para avisar sobre la cercanía del plazo de cancelación Implantar mecanismos de cancelación y en su caso el bloqueo de datos
Datos especialmente protegidos	Fallos o errores sistemáticos u ocasionales para recabar consentimiento expreso para el tratamiento o cesión	Evitar el tratamiento de datos especialmente protegidos salvo que sea imprescindible para la finalidad Establecer procedimientos que garanticen la obtención del consentimiento expreso o por escrito
	Asunción errónea de la existencia de habilitación legal para el tratamiento o cesión	Nombrar a un DPO para contar con asesoramiento especializado
	Fallos para recabar el consentimiento expreso para el tratamiento o para la cesión	Utilizar técnicas de disociación
Deber de secreto	Puede existir algún acceso no autorizado	Concienciación sobre el deber de secreto Establecer sanciones disciplinarias por violación del deber de secreto y políticas de confidencialidad Establecer procedimientos para garantizar la notificación del deber de secreto y consecuencias de su incumplimiento Notificar que se dará traslado a las autoridades de incumplimientos que conlleven consecuencias penales Establecer procedimientos para la destrucción de soportes con datos personales
	Violaciones de confidencialidad de los datos personales por parte de los empleados	Formación adecuada de los empleado Establecimiento de sanciones disuasorias

TIPOLOGÍA	DESCRIPCIÓN DEL RIESGO	MEDIDA
Tratamientos por encargo	Inexistencia de contrato o elaboración del contrato incorrecto que no refleje todos los apartados necesarios o las garantías adecuadas	Establecer procedimientos para que existan contratos con los encargados que contemplen la PD
	Falta de diligencia en la elección del encargado del tratamiento	Seleccionar encargados que garanticen el cumplimiento normativo Establecer mecanismos de control a encargados
	Gestión deficiente de subcontrataciones o incorrecto seguimiento de la contratación	Establecer mecanismos que garanticen el control sobre las actividades de subcontratistas Realizar auditorías periódicas al encargado Definir Acuerdos de Nivel de Servicio
	No definición o deficiencias en los procedimientos para comunicar al responsable los derechos ARCO	Incluir en el contrato la obligación de informar de los derechos arco Definir procedimientos claros de comunicación de estas solicitudes de derechos
	Dificultades para conseguir la portabilidad de los datos	Incluir la obligación de portabilidad en los contratos Establecer las medidas técnicas y organizativas para garantizar la portabilidad
Derechos ARCO	Dificultar o imposibilitar el ejercicio de los derechos ARCO	Implantar sistemas que permitan fácilmente a los afectados el acceso a sus datos y el ejercicio de sus derechos Evitar ejercicio de derechos no gratis Evitar procedimientos poco claros y laboriosos Formar al personal para que conozca como satisfacer derechos Definir quien se encarga de contestar al ejercicio de derechos
	Carencia de procedimientos y herramientas para la gestión de los derechos ARCO	Definición de procedimientos para el ejercicio de derechos Formación al personal que debe gestionarlos
	Carencia de procedimientos para comunicar rectificaciones, cancelaciones u oposiciones a los cesionarios de datos personales	Definición de procedimientos de comunicación del ejercicio de derechos arco a organizaciones a las que se han cedido Establecimiento de acuerdos con los cesionarios para garantizar la correcta actualización de datos Formación al personal que debe gestionarlos

Tratamiento de los riesgos de seguridad

Respecto a las medidas que se pueden implementar a la hora de tratar los riesgos a la seguridad de los datos, dado que los riesgos identificados en la fase anterior están relacionados con los dominios, el tratamiento será la implementación de los controles asociados a esos dominios. En este apartado habrá que tener en cuenta que algunos controles no se implantarán puesto no son aplicables al tratamiento objeto del EIPD.

El conjunto de medidas correspondientes a la seguridad es el siguiente (3):

RIESGO ASOOCIADO AL DOMINIO	MEDIDA
Políticas de seguridad	5.1.1 política de seguridad de la información 5.1.2 Revisión de las políticas de seguridad de la información

RIESGO ASOOCIADO AL DOMINIO	MEDIDA
Organización de la Seguridad	6.1.1 Roles y responsabilidades en seguridad de la información 6.1.2 Segregación de tareas 6.1.3 Contacto con las autoridades 6.1.4 Contacto con grupos de interés especial 6.1.5 Seguridad de la información en la gestión de proyectos 6.2.1 Política de dispositivos móviles 6.2.2 Teletrabajo
Seguridad relativa a los recursos humanos	7.1.1 Investigación de antecedentes 7.1.2 Términos y condiciones del empleo 7.2.1 Responsabilidades de gestión 7.2.2 Concienciación, educación y capacitación en seguridad de la información 7.2.3 Proceso disciplinario 7.3.1 Responsabilidades ante la finalización o cambio
Gestión de activos	8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.1.3 Uso aceptable de los activos 8.1.4 Devolución de activos 8.2.1 Clasificación de la información 8.2.2 Etiquetado de la información 8.2.3 Manipulado de la información 8.3.1 Gestión de soportes extraíbles 8.3.2 Eliminación de soportes 8.3.3 Soportes físicos en tránsito

RIESGO ASOOCIADO AL DOMINIO	MEDIDA
Control de accesos	9.1.1 Política de control de acceso 9.1.2 Acceso a las redes y a los servicios de red 9.2.1 Registro y baja de usuario 9.2.2. Provisión de acceso de los usuarios 9.2.3 Gestión de privilegios de acceso 9.2 4 Gestión de la información secreta de autentificación de los usuarios 9.2.5 Revisión de los derechos de acceso de usuario 9.2.6 Retirada o reajuste de los derechos de acceso 9.3.1 Uso de la información secreta de autenticación 9.4 Control de acceso a sistemas y aplicaciones 9.4.1 Restricción del acceso a la información 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Sistema de gestión de contraseñas 9.4.4 Uso de utilidades con privilegios del sistema 9.4.5 Control de acceso al código fuente de los programas
Criptografía	10.1.1 Política de uso de los controles criptográficos 10.1.2 Gestión de claves
Seguridad física y del entorno	11.1.1 Perímetro de seguridad física 11.1.2 Controles físicos de entrada 11.1.3 Seguridad de oficinas, despachos y recursos 11.1.4 Protección contra las amenazas externas y ambientales 11.1.5 El trabajo en áreas seguras 11.1.6 Áreas de carga y descarga 11.2.1 Emplazamiento y protección de equipos 11.2.2 Instalaciones de suministro 11.2.3 Seguridad del cableado 11.2.4 Mantenimiento de los equipos

RIESGO ASOOCIADO AL DOMINIO	MEDIDA
	11.2.5 Retirada de materiales propiedad de la empresa 11.2.6 Seguridad de los equipos fuera de las instalaciones 11.2.7 Reutilización o eliminación de equipos 11.2.8 Equipo de usuario desatendido 11.2.9 Política de puesto de trabajo despejado y pantalla limpia
Seguridad de las operaciones	12.1.1 Documentación de procedimientos de la operación 12.1.2 Gestión de cambios 12.1.3 Gestión de capacidades 12.1.4 Separación de los recursos de desarrollo, prueba y operación 12.2.1 Controles contra el código malicioso 12.3.1 Copias de seguridad de la información 12.4.1 Registro de eventos 12.4.2 Protección de la información de registro 12.4.3 Registros de administración y operación 12.4.4 Sincronización del reloj 12.5.1 Instalación del software en explotación 12.6.1 Control de las vulnerabilidades técnicas 12.6.2 Restricción en la instalación de software 12.7.1 Control de auditoría de sistemas de información
Seguridad en las comunicaciones	13.1.1 Controles de red 13.1.2 Seguridad de los servicios de red 13.1.3 Segregación en redes 13.2.1 Políticas y procedimientos de intercambio de información 13.2.2 Acuerdos de intercambio 13.2.3 Mensajería electrónica 13.2.4 Acuerdos de confidencialidad

RIESGO ASOOCIADO AL DOMINIO	MEDIDA
Adquisición, desarrollo y mantenimiento de sistemas de información	14.1.1 Análisis de requisitos y especificaciones de Seguridad de la información 14.1.2 Asegurar los servicios de aplicaciones en redes públicas 14.1.3 Protección de las transacciones de servicios de aplicaciones 14.2.1 Política de desarrollo seguro 14.2.2 Procedimiento de control de cambios en sistemas 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 14.2.4 Restricciones a los cambios en los paquetes de software 14.2.5 Principios de ingeniería de sistemas seguros 14.2.6 Entorno de desarrollo seguro 14.2.7 Externalización del desarrollo de software 14.2.8 Pruebas funcionales de seguridad 14.2.9 Pruebas de aceptación de sistemas 14.3.1 Protección de los datos de prueba
Relación con proveedores	15.1.1 Política de seguridad de la información en relaciones con los proveedores 15.1.2 Requisitos de seguridad en contratos con terceros 15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones 15.2 1 Supervisión y revisión de los servicios prestados por terceros 15.2.2 Gestión de cambios en los servicios prestados por terceros
Gestión de incidentes de seguridad de la información	16.1.1 Responsabilidades y procedimientos 16.1.2 Notificación de los eventos de seguridad de la información 16.1.3 Notificación de puntos débiles de la seguridad 16.1.4 Evaluación y decisión sobre los eventos de seguridad de información 16.1.5 Respuesta a incidentes de seguridad de la información 16.1.6 Aprendizaje de los incidentes de seguridad de la información 16.1.7 Recopilación de evidencias

RIESGO ASOCIADO AL DOMINIO	MEDIDA
Aspectos de seguridad de la información para la gestión de la continuidad del negocio	17.1.1 Planificación de la continuidad de seguridad de la información 17.1.2 Implementar la continuidad de la seguridad de la información 17.1.3 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio 17.2.1 Disponibilidad de instalaciones de tratamiento de la información
Cumplimiento	18.1.1 Identificación de la legislación aplicable 18.1.2 Derechos de propiedad intelectual (DPI) 18.1.3 Protección de los registros de la organización 18.1.4 Protección de datos y privacidad de la información de carácter personal 18.1.5 Regulación de los controles criptográficos 18.2.1 Revisión independiente de la seguridad de la información 18.2.2 Cumplimiento de las políticas y normas de seguridad 18.2.3 Comprobación del cumplimiento técnico

Las medidas a implantar vendrán dadas por el análisis de riesgos realizado por el equipo de seguridad.

Análisis de cumplimiento normativo

En esta fase se verificará que el tratamiento que es objeto del EIPD da cumplimiento a las normas legales que le son de aplicación.

En este caso habrá que identificar cuáles son estas normas y se tendrán en cuenta si recogen requisitos de protección de datos. Para este proyecto se considerará que no existe ninguna legislación sectorial aplicable al tratamiento que refleje este tipo de requisitos.

Dado que la Guía de la AEPD, en su anexo I, incluye una serie de preguntas para realizar este análisis, este cuestionario será el que se refleje en la solución propuesta (4):

LEGITIMACIÓN DE LOS TRATAMIENTOS

¿Se cuenta con el consentimiento libre, específico, inequívoco e informado de los afectados para el tratamiento de sus datos?

En caso contrario:
- ¿está autorizado por una Ley?
- ¿se deriva del ejercicio de competencias propias de las AAPP?
- ¿responde a una relación negocial, contractual, laboral o administrativa?
- ¿se debe a un interés vital del afectado?
- ¿proceden los datos de fuentes accesibles al público?
- ¿es necesario para la satisfacción del interés legítimo del responsable del fichero siempre que no prevalezca el interés derecho o libertades del interesado? En este caso, ¿se ha realizado un análisis y ponderación de estos derechos?
- ¿está asociado al ejercicio de un derecho fundamental? ¿prevalece sobre el derecho a la protección de datos?

En el caso de que el tratamiento se base en el consentimiento ¿existen mecanismos para garantizar que su recogida es conforme a la Ley y se puede revocar?

LEGITIMACIÓN DE LAS CESIONES DE DATOS PERSONALES

¿Se cuenta con el consentimiento libre, específico, inequívoco e informado de los afectados para la cesión de sus datos?

En caso contrario:
- ¿está autorizado por alguna Ley?
- ¿se deriva de libre y legítima aceptación de una relación jurídica que la exija?
- ¿es para el Defensor del Pueblo, Ministerio Fiscal, Jueces o Tribunales o Tribunal de Cuentas u organismos autónomos similares?
- ¿Se realiza entre AAPP para competencias similares o tratamiento con fines estadísticos, científicos o históricos?
- ¿es necesaria para solucionar una urgencia o para estudios epidemiológicos?
- ¿proceden los datos de fuentes accesibles al público?
- ¿es necesario para la satisfacción del interés legítimo del responsable del fichero siempre que no prevalezca el interés derecho o libertades del interesado? En este caso, ¿se ha realizado un análisis y ponderación de estos derechos? ¿se han establecido medidas de garantía y salvaguarda para limitar los efectos de la cesión sobre los afectados?

¿Se informa de la finalidad a la que se destinan los datos o tipo de actividad del cesionario?

¿Se está en condiciones de acreditar el consentimiento obtenido?

¿Se ha habilitado procedimiento para la revocación del consentimiento?

TRANSFERENCIAS INTERNACIONALES

¿Se van a transmitir datos personales fuera de España?

¿Es el país destino miembro de la UE?

Si no es así ¿es adecuado por la CE o la Directora de la AEPD?

En caso contrario ¿se puede aplicar excepciones del art. 34?

Si no es ningún caso anterior ¿se ha solicitado autorización a la Directora?

Si se trata de un encargo de tratamiento que desea subcontratar a terceros países ¿se utilizan las cláusulas adecuadas? En caso contrario ¿cada responsable solicita su correspondiente autorización?

NOTIFICACIÓN DE LOS TRATAMIENTOS A LA AEPD
¿Se ha seguido los pasos para la notificación al RGPD del tratamiento? En caso de ser AAPP, ¿se ha publicado la disposición de carácter general?
TRANSPARENCIA DE LOS TRATAMIENTOS
¿Se informa a los afectados expresa e inequívocamente de lo reflejado en el art. 5? ¿La información anterior ¿está en todos los formularios? Si lo datos no se recaban del afectado ¿se informa a los mismos en el plazo de 3 meses de lo previsto en el art. 5?
CALIDAD DE LOS DATOS
¿Se recogen solo los datos estrictamente necesarios para las finalidades del tratamiento? ¿Se recaban los datos de forma leal y transparente? ¿Se usan los datos para finalidades distintas o incompatibles con las declaradas? ¿Se adoptan las garantías necesarias para el tratamiento con finalidades históricas, científicas o estadísticas? ¿Existen mecanismos de actualización de datos y verificación de dicha actualización? ¿Se contempla la posibilidad de cancelar los datos de oficio, cuando ya no sean necesarios? ¿Se definen plazos de conservación de los datos? ¿Existen procedimientos para determinar cuándo cumplen dichos plazos? ¿Se conservan los datos de forma que facilitan el ejercicio de derechos arco? En caso de datos disociados ¿se utilizan procedimientos que garantizan la irreversibilidad del proceso y la imposibilidad de re identificación?
DATOS ESPECIALMENTE PROTEGIDOS
Si se tratan datos de ideología, creencias, religión o afiliación sindical ¿se cuenta con consentimiento expreso y por escrito? Si se tratan datos de salud, vida sexual u origen racial o étnico ¿se cuenta con consentimiento expreso? En caso contrario ¿existe alguna Ley que lo permita? ¿Se puede acreditar el consentimiento obtenido? ¿Se han habilitado procedimientos para gestionar la revocación del consentimiento ¿ ¿Se recogen datos de infracciones penales o administrativas sin ser órgano competente? En caso de tratamientos para la prestación o gestión de servicios sanitarios ¿se garantiza el deber de secreto? ¿Se limita el acceso a los datos de salud a los estrictamente necesarios a cada role?

DEBER DE SECRETO

¿Se forma adecuadamente a todo el personal de la obligación de guardar secreto?

¿Se les informa adecuadamente de las obligaciones y consecuencias de no hacerlo? ¿Queda constancia de dicha información?

TRATAMIENTOS POR ENCARGO

¿Se ha realizado el análisis adecuado para la selección del encargado?

¿Existe un contrato con las garantías legales?

¿Se han adoptado medidas para verificar el cumplimiento de las condiciones del contrato y medidas de seguridad por parte del encargado o posibles subcontratistas?

¿Se estipula que el encargado solo accederá a los datos conforme a las instrucciones del responsable?

¿Se estipula que los datos no serán comunicados a otras personas?

¿Se estipulan que las medidas de seguridad que debe adoptar el encargado?

¿Se regula el destino de los datos al finalizar el encargo?

¿Se informa al encargado que en caso de incumplimiento será considerado responsable y podrá ser sancionado?

¿Existe una cesión porque el encargado establece un nuevo vínculo con los afectados?

Si existen subcontrataciones ¿se cuenta con la autorización del responsable?

Si no existe esa autorización ¿se han especificado en el contrato los servicios que pueden ser subcontratados y la empresa a subcontratar? En su defecto ¿se comunica al responsable la empresa subcontratada cuando esta se produzca? ¿Se formaliza contrato entre encargado y subcontratista?

Si el encargado presta sus servicios en los locales del responsable o accede de forma remota a sus sistemas sin posibilidad de copiar datos ¿se refleja este hecho en los documentos de seguridad del responsable? ¿Se ha comprometido el personal del encargado a cumplir con las medidas de seguridad?

Si el encargo no implica acceso a datos ¿se recoge esta prohibición y la obligación de secreto en caso de acceso accidental?

Si el servicio se presta en los locales del encargado ¿se ha incluido este hecho en la documentación de seguridad del responsable? ¿Lo contempla el encargado en su propia documentación de seguridad?

DERECHOS ARCO

¿Se han adoptado las medidas necesarias para garantizar el carácter personalísimo del ejercicio de derechos?

¿Se han adoptado las medidas para acreditar la representación en casos de incapacidad o minoría de edad?

¿Se ha previsto el ejercicio de derechos ARCO mediante representante voluntario y la forma de acreditar dicha representación?

Si el responsable dispone de servicios de atención al público ¿se pueden utilizar para ejercer los derechos ARCO y se considera acreditada la identidad de los interesados mediante los medios establecidos por el responsable para la prestación

de estos servicios? ¿Se conservan los datos de forma que permitan un fácil y rápido ejercicio de derechos? ¿Se han implantado las medidas y procedimientos adecuados para garantizar los plazos marcados por la ley? En el caso de existir encargado ¿se le ha instruido para que den traslado de cualquier ejercicio de derechos que reciban? ¿Se han implantado las medidas de y procedimientos adecuados para siempre contestar al interesado? ¿Existen mecanismos u/y procedimientos para informar a los posibles cesionarios de rectificaciones o cancelaciones? En el caso de derecho de acceso ¿se ofrece toda la información que establece la ley de forma adecuada? ¿Se garantiza que el derecho se pueda ejercer en plazos superiores a 12 meses o cuando se acredite interés legítimo? En el caso de derecho de cancelación ¿se conservan los datos sólo y exclusivamente durante el plazo obligatorio? ¿Se mantienen los datos bloqueados a disposición de AAPP, jueces y tribunales durante el plazo de responsabilidad? En el caso de que se adopten decisiones con efectos jurídicos basadas únicamente en tratamientos automatizados ¿existen mecanismos que posibiliten la impugnación de estas decisiones? ¿Existen procedimientos para dar información sobre los criterios de valoración y el programa utilizado para ello?

Análisis de cumplimiento normativo de seguridad

El análisis de cumplimiento normativo de la parte de seguridad, al basarnos en el nuevo reglamento que no detalla requisitos de seguridad a implantar y solo implica que se implanten medidas de seguridad en base a un análisis de riesgos, a efectos de este proyecto el análisis de cumplimiento de este aspecto se realizará en genérico (3):

SEGURIDAD
¿Existe un análisis de riesgos? ¿Se han implantados los controles adecuados para el tratamiento de los riesgos identificados?

Elaboración del Informe definitivo

El informe definitivo a presentar al Responsable del fichero o tratamiento, constará, al menos, de los siguientes apartados:

- Datos identificativos del informe:
    - Nombre del informe
    - Código
    - Fecha
    - Versión
    - Autor

- Resumen ejecutivo
    - Objeto del informe
    - Breve justificación de la necesidad del informe
    - Descripción breve del tratamiento
    - Principales riesgos identificados
    - Principales medidas para tratar los principales riesgos
- Descripción detallada del proyecto
- Identificación de riesgos
- Medidas implantadas
- Análisis de cumplimiento normativo
    - Deficiencias detectadas
    - Recomendaciones propuestas
- Conclusiones

Implantación de recomendaciones

Esta fase será realizada por el responsable del fichero o tratamiento, aunque dependiendo de la organización, cada una de las recomendaciones podrán ser asignadas a distintos equipos de trabajo de diferentes departamentos en base a sus competencias.

Revisión y mantenimiento del EIPD

En esta última fase se deberá realizar una revisión de la eficacia del Informe, es decir, si el tratamiento, una vez implantadas las recomendaciones del informe, ha logrado el objetivo marcado en el documento.

También esta fase incorpora un mantenimiento del propio informe, ya que si se produce una modificación en algunos de los aspectos que han servido de base para la realización del informe, este tendrá que ser actualizado en base a dicha modificación. También habrá que tener en cuenta que este mantenimiento del informe se deberá realizar si el tratamiento sufre otra modificación sustancial que implique esta necesidad, según la tabla de la primera fase de la metodología.

De esta forma, se cierra el ciclo de mejora continua en el que se basa este proyecto.

8.2 Segunda parte: Herramienta web

Con el objetivo de plasmar de una manera más visible esta metodología y que distintas empresas puedan completar la EIPD de una manera más sencilla se ha procedido a crear una herramienta.

8.2.1 Descripción del entorno tecnológico

El primer dilema que se presenta es en cuanto al formato de la herramienta, y si ésta debe ser on premise o en cloud. Con el objetivo de llegar al mayor público posible y acceder a esta herramienta de una manera rápida y sencilla, y que no exista la necesidad de almacenar documentos o programas en la memoria del ordenador, se ha decidido utilizar un formato web.

Elección y modificaciones de la plantilla

Ya que el objetivo es la realización de una herramienta Web sencilla pero con una apariencia amistosa que resulte útil, se ha procedido a utilizar un template con un diseño sencillo, modificado para cubrir las necesidades de la metodología.

Requisitos importantes en la búsqueda de template:

1. Uso de tecnologías conocidas (html, css, javascript, php…).
2. Menú de navegación permanente.
3. Separación en módulos.
4. Diseño sencillo con líneas limpias.
5. Diseño que permita comparativas de a dos.
6. Responsive.

Una vez encontrada la plantilla deseada, lo primero es ver qué módulos encajan en cada parte de la metodología, en este caso, se ha utilizado una división en dos cajas para separar la protección de datos de la seguridad, desplegables para las ideas del análisis de la necesidad y elementos estáticos para los últimos puntos y la primera imágen de la metodología (9).

Una vez adaptados estos elementos al contenido de la metodología, pasamos a las customizaciones del diseño. Comenzando con el uso de imágenes, obtenidas de un banco de imágenes gratuitas y editadas usando el programa GIMP, y siguiendo con el uso de colores corporativos de la UCM (blanco y granate).

Elección de herramienta de formularios

Una vez se ha procedido a crear el grueso de la web, se procede a crear una herramienta para la extracción del informe de las medidas necesarias para la EIPD. Al comenzar surgen diferentes dudas:

- ¿Es necesario el uso de una base de datos? No, ya que ni se manejan grandes cantidades de datos, ni hay información estructurada ni niveles de seguridad. Por otro lado no se espera que el sitio cambie frecuentemente ni el contenido es User-Driven.
- ¿Es mejor utilizar PHP o Javascript para obtener el PDF? Por conocimiento del lenguaje y sencillez, se ha decido usar Javascript para escribir en fichero.

Una vez se ha llegado a estas conclusiones, se ha construido una pequeña herramienta que a través de un formulario, de riesgos en caso de protección de datos y de medidas en seguridad, muestra las medidas que han de ser incorporadas al informe final (10) (11) (12).

8.2.2 Diseño Web

Página inicial

El diseño aborda el título del proyecto junto a un menú o barra de navegación

- Barra de navegación: La barra de navegación contiene como primer elemento, situado a la izquierda, el icono de la Universidad Complutense de Madrid. A continuación aparece el menú de navegación, con cada uno de los subapartados de los que consta la Web.
- Título: La sección que define el título contiene una imagen y el título del proyecto. El título también contiene un botón hace referencia a comenzar con la metodología.

Introducción a la metodología

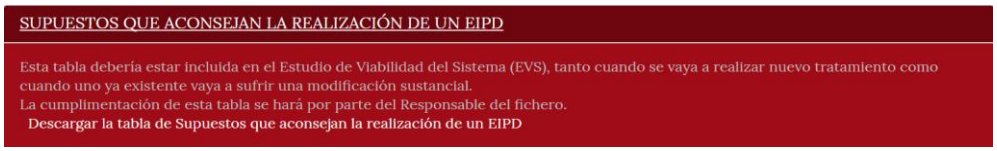
La siguiente sección incluye la barra de navegación que será recurrente durante las distintas secciones que contiene la página web. En este punto se explica la metodología propuesta, para ello, se muestra el diagrama de la parte de introducción a la metodología, que consta de los pasos que la forman. Al sobrevolar esta imagen con el mouse, aparece un texto explicativo con el objetivo de esta metodología.

Pasos de la metodología

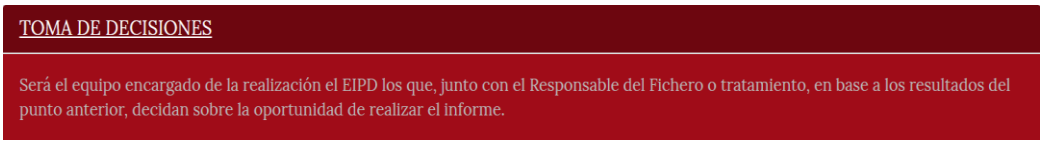
Las secciones posteriores contienen los distintos pasos que se deben seguir para la consecución de la EIPD.

- **Evaluación:** En esta parte ayuda al usuario a tomar una valorar la necesidad o no de realizar la EIPD. Para ello consta de varios desplegables, que indican:
    - Necesidad de realización de un EIPD: En este apartado hay una pequeña introducción que contextualiza al Usuario en este primer paso de la EIPD.

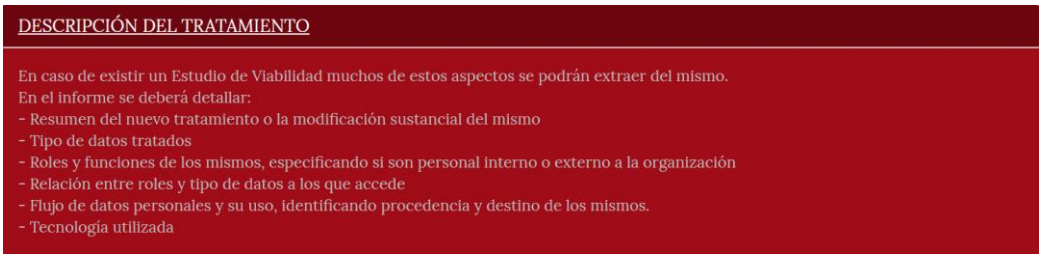
- Supuestos que aconsejan la realización de un EIPD: Este apartado contiene un enlace de descarga que contiene la Tabla de supuestos.



- Toma de Decisiones: Después de que el Responsable del Fichero o Tratamiento complete la tabla, el equipo de Protección de datos junto al responsable del fichero debe valorar la necesidad de realizar una EIPD.
  NOTA: En un futuro, la autoridad competente (En este caso la Agencia Española de Protección de Datos) será la que concrete los supuestos en los que la realización de esta evaluación será obligatoria.



- Descripción del Tratamiento: En este apartado, el Usuario debe recoger las conclusiones obtenidas tras el análisis de los supuestos anteriores, junto a una breve descripción del tratamiento, proporcionada por parte del Responsable del Tratamiento, en caso de que exista previamente un Estudio de Viabilidad del Sistema (EVS), esta información se puede obtener del mismo.



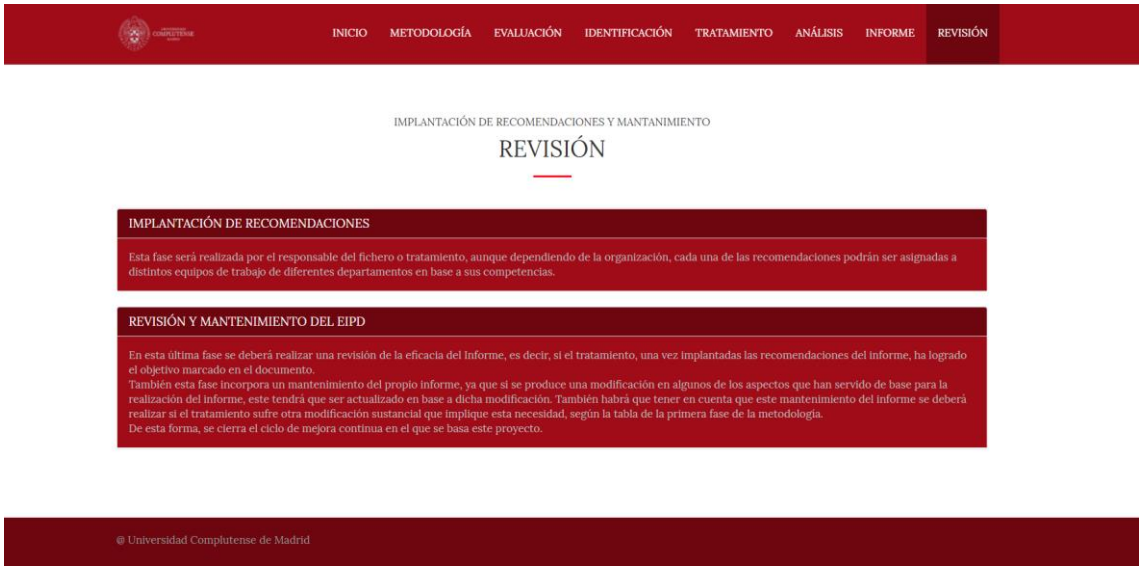
- **Identificación**: En este apartado se orienta al Usuario acerca de los pasos que seguir para realizar el análisis de riesgos del sistema. Consta de una breve introducción y dos subapartados claramente diferenciados. En el caso del apartado de protección de datos, el análisis ha de hacerse en base a la tabla descargable en este punto (Tabla 2) por parte del equipo de protección de datos, sin embargo, en el subapartado de seguridad, el usuario debe pedir la identificación de los riesgos al Equipo de seguridad TIC y se ha de hacer por medio de una herramienta externa.

- **Tratamiento**: Este punto, al igual que el anterior, se divide en una introducción y dos subapartados. Ambos contienen enlaces a formularios externos con los que se obtienen las medidas a aplicar, que serán explicados posteriormente.

- **Análisis**: En este punto, el equipo de protección de datos debe completar las tablas descargables tanto en materia de protección de datos como en materia de seguridad. Tomando estas tablas como ayuda, es necesario analizar si el tratamiento cumple con la normativa vigente.

- **Informe**: En este punto se resumen los distintos apartados y la información que ha de tener el informe definitivo y que el usuario ha debido recolectar utilizando los puntos anteriores de la metodología.

- **Revisión**: Tras la obtención del informe definitivo, el equipo de protección de datos debe implantar las recomendaciones, revisar su efectividad y, en caso de que la legislación o el tratamiento cambie, volver a implantar la metodología. De esta forma se cierra el circo que conforma esta metodología.



Formularios

Con el objetivo de ayudar al usuario a la realización del informe final, se han realizado dos formularios para obtener las medidas necesarias para el tratamiento de datos. La web contiene un formulario dividido en secciones que se localizan en un carrusel, cada una de las secciones tiene en diversos checkbox que el usuario ha de marcar con los resultados del análisis de riesgos

- **Protección de datos:** Tras la realización del análisis de riesgos de protección de datos, el usuario debe dar click en todos los riegos detectados en el mismo. El programa devuelve en formato pdf las medias necesarias, como se explica en la tabla del apartado 8.1.3, en cuanto a la protección de datos, hay una relación directa entre los riesgos y las medidas que se han a tomar.

- **Seguridad de datos:** En el caso de la parte de seguridad de la información, el análisis de riesgos que se hace de una manera externa reporta directamente las medidas, por lo que en el programa sólo habría que confirmar cada una de ellas según al dominio al que pertenezcan, para obtener el pdf.

Ejemplo de una página del formulario, como se puede ver la página consta de un título y clasifica por los distintos riesgos:

En la parte de seguridad se indican las medidas que se obtienen en el análisis de riesgos.

Para obtener las medidas hay que hacer click en el botón y descargar:

Éste es el pdf que se obtiene con las Medidas a implantar:

INFORME DE PROTECCIÓN DE DATOS

Médidas a implantar tras el análisis de Riesgos Generales:

Formación al personal en PD
Comunicación clara y auditable de las responsabilidades relacionadas con el cumplimiento y con las consecuencias en caso de incumplimiento
Formación al personal en PD a nivel sectorial
Comunicación clara y auditable de las responsabilidades relacionadas con el cumplimiento (sectorial) y con las consecuencias en caso de incumplimiento
Formación al personal en Seguridad y uso de las TIC
Comunicación clara y auditable de las responsabilidades relacionadas con el cumplimiento de políticas y normas de seguridad y con las consecuencias en caso de incumplimiento
Formación al personal en PD, Seguridad y uso de las TIC
Nombramiento para la interlocución con los afectados
Nombrar a un Delegado de Protección de Datos (DPO), que también puede hacer de interlocutor
Incorporación de privacidad en el diseño
Incorporación DPO

Médidas a implantar tras el análisis de Legitimación de tratamientos y cesiones:

Usar datos disociados
Si se puede, utilizar el uso de anónimos
Revisar la existencia de datos personales no utilizados
Utilizar pseudónimos
Evitar el uso de datos biométricos
Verificar que el tratamiento de datos especialmente protegidos es imprescindible para la finalidad
Verificar que el tratamiento está amparado por la Ley
En caso contrario garantizar que se obtienen el consentimiento expreso o por escrito
Evitar uso de cookies u otros mecanismos de rastreo y monitorización, si se utilizan escoger las menos invasivas
Informar sobre el uso y finalidad de las cookies
Respetar las preferencias de los afectados en sus navegadores
Permitir uso anónimo de servicios y productos cuando no sea necesario la identificación de las personas

Médidas a implantar tras el análisis de Transferencias internacionales:

Incluir cláusulas de salvaguarda en las que se refiera información sobre los accesos a datos transferidos tan pronto como sea posible
Implantar mecanismos de control para garantizar que se cumplen las condiciones bajo las que se llevó a cabo la transferencia
Asegurarse de la exigencia de mecanismos de control del importador
Asegurarse de la definición y funcionamiento de un canal de comunicación para las solicitudes y reclamaciones
Poner en marcha procedimientos que garanticen la adecuada atención de las demandas
Solicitar autorización de la Directora de la AEPD si es necesario

9. Conclusiones

Este proyecto aporta una solución a una realidad que se plantean muchas organizaciones. Presenta un aspecto innovador al integrar, en una misma metodología de evaluación de impacto, la protección de datos y la seguridad de éstos, y proporcionar una herramienta ágil para obtener una solución global en estas dos materias a organizaciones públicas y privadas. Esta solución podría ser utilizada en los países pertenecientes a la Unión Europea ya que las normativas que integra, protección de datos y seguridad de la información, la primera es de obligado cumplimiento y la segunda un estándar de facto a nivel internacional cuya adopción está muy extendida.

El valor añadido que presenta el proyecto, es que la metodología creada es válida si se sustituye el marco de control de la Norma ISO/IEC 27002 por cualquier otro marco de controles de seguridad, por ejemplo, en el caso de la Administración Pública Española, se podría tomar de referencia las medidas de seguridad establecidas por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, norma legal de obligado cumplimiento para todo el Sector Público a nivel nacional, autonómico y local.

10. Conclusion

This project brings a solution to a reality that many organizations have. It presents innovation by integrating data protection and data security into a single impact assessment methodology, and providing an agile tool to obtain a global solution in these two areas to public and private organizations. This solution could be used in the countries belonging to the European Union since the regulations that integrate, data protection and information security, the first one is mandatory and the second one is a de facto standard at international level which adoption is widespread.

The added value of the project is that the methodology created is valid if the control framework of ISO / IEC 27002 is replaced by any other framework of safety controls, for example in the case of the Spanish Public Administration, the reference could be the security measures established by Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of electronic administration, a mandatory legal norm for the entire Sector Public at national, regional and local levels.

11. Bibliografía

1. ***Norma Internacional ISO/IEC 27001:2013.*** **2013.**

2. ***Norma Internacional ISO/IEC 27002:2013.*** **2013.**

3. Europeo, Parlamento. ***REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.*** **s.l. : Parlamento Europeo, 2016.**

4. AEPD, Agencia Española de Protección de Datos. Guía de la Agencia Española de Protección de datos. [En línea] https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf.

5. Fundación Wikimedia, Inc. Wikipedia.org. [En línea] https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo.

6. ***Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.*** **15, 1999.**

7. ***Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.*** **BOE : s.n., 2007.**

8. Protegete.jccm.es. [En línea] http://protegete.jccm.es/protegete/opencms/Administracion/Curso_LOPD/Ampliacion_Curso/curso.html.

9. Themewagon.com. [En línea] https://themewagon.com/themes/free-lawyer-attorney-website-bootstrap-html5-template/.

10. Fuente 1 javascript. [En línea] http://codeactually.com/interactivequiz.html.

11. Fuente 2 javascript. [En línea] https://desarrolloweb.com/articulos/995.php.

12. Fuente 3 javascript. [En línea] https://www.youtube.com/watch?v=_EqYMNdbrsc.

13. Pixabay. ***Banco de imágenes.*** **[En línea] https://pixabay.com/es/.**